



وزارة التعليم
Ministry of Education

الوحدة الأولى الدرس الأول



الأمن السيبراني



من المقرر ثالث متوسط

الفصل الدراسي الأول ١٤٤٨هـ



وزارة التعليم
Ministry of Education

بيانات الدرس



صفحات الكتاب

الحصة الأولى

من صفحة: 13

إلى صفحة: 16



عدد الحصص

حصتان



عنوان الدرس

مقدمة في الأمن
السيبراني



رقم الدرس

الدرس الأول



وزارة التعليم
Ministry of Education

من خلال عنوان الدرس

مقدمة في الأمن السيبراني

نقوم بتعبئة الخانتين على اليمين



كيف أتعلم المزيد؟



ماذا تعلمت؟



ماذا أريد أن أعرف؟



ماذا أعرف؟



وزارة التعليم
Ministry of Education

الإستراتيجيات





وزارة التعليم
Ministry of Education



تمهيد الدرس

66 الوحدة الأولى / الدرس الأول

مقدمة في الأمن السيبراني

- ❖ ماذا نعني بمفهوم الأمن السيبراني؟
- ❖ هل سبق أن سمعتم بتعرض أحد لاختراق حساباته في مواقع التواصل الاجتماعي؟
- ❖ ما المقصود بالجرائم الإلكترونية؟ من هم الأفراد أو الكيانات المتورطة فيه؟
- ❖ من منكم يستخدم التحقق الثنائي لحماية حساباته على الإنترنت؟
- ❖ هل قمت بتفعيل التحقق الثنائي في منصة مدرستي؟

ميّار والاختراق الصامت

في اللحظة التي بدأت فيها ميّار تدريبيًا افتراضيًا، انطفأت مدينة «سيبرون» وظهرت ثلاثة مؤشرات حمراء: السرية، والتكامل، والتوافر.

أدركت أن مهاجمًا يحاول تعطيل الشبكة وسرقة بيانات السكان.

راجعت السجلات، فاكتشفت رسالة تصيد قادت إلى اختراق أمني، ثم لاحظت أن بعض الملفات عُدلت وأن الخدمات بدأت تتوقف.

فعلت التحقق المتعدد، وأغلقت الحسابات المشبوهة، واستعادت نسخة احتياطية، ثم حدثت الأنظمة وشغلت جدار الحماية.

عادت المدينة تدريجيًا، لكن بقي سؤال أخير على الشاشة: «هل كان الهجوم خارجيًا حقًا؟».

خرجت ميّار وهي تدرك أن الأمن السيبراني ليس برنامجًا واحدًا، بل منظومة وعي وحماية مستمرة.

ميّار والاختراق الصامت





وزارة التعليم
Ministry of Education



حيث يساعدنا في حماية
حساباتنا وملفاتنا الشخصية

وتطوير الوعي الأمني الرقمي



النشاط الاثرائي





وزارة التعليم
Ministry of Education

مفردات الدرس

1. الأمن السيبراني
2. مثلث الحماية CIA
3. الجرائم الإلكترونية
4. الاختراق الأمني



ماذا سنتعلم ؟



وزارة التعليم
Ministry of Education

ماهية
الاختراق
الأمني.

أنواع الجرائم
الإلكترونية.

الجرائم
الإلكترونية.

مثلث الحماية
CIA.

أهمية الأمن
السيبراني.

الأمن
السيبراني.



وزارة التعليم
Ministry of Education

رَبِّطْ بِالْوَطَنِ

في المملكة العربية السعودية، تسعى الهيئة الوطنية للأمن السيبراني إلى تعزيز الأمان السيبراني من خلال برنامج "ساير"، الذي يركز على حماية البيانات الحكومية والشخصية من التهديدات الإلكترونية. يتضمن البرنامج تنفيذ استراتيجيات متقدمة مثل مراقبة الشبكات وتحليل التهديدات، وتدريب موظفي الحكومة على أفضل ممارسات الأمن السيبراني، لضمان سلامة المعلومات الحساسة وحماية الثقة في الأنظمة الرقمية من خلال الاستجابة الفعّالة للهجمات الإلكترونية.



مخصر الدرس





وزارة التعليم
Ministry of Education



ورقة العمل



عرض محتوى الكتاب

الأمن السيبراني:



يتعلق مفهوم الأمن السيبراني بحماية أجهزة الحاسب والشبكات والبرامج والبيانات من الوصول غير المصرح به، والذي قد يهدف إلى الحصول على المعلومات الحساسة أو تغييرها أو إتلافها أو ابتزاز المستخدمين للحصول على الأموال، بل وأحياناً تعطيل عمليات المؤسسة عمومًا. يُعبّر مصطلح الأمن السيبراني عن جميع الممارسات التي تتم لحماية المعلومات من المخاطر والهجمات التي تتمثل في الوصول غير المصرح به بغرض الاستخدام غير المشروع أو التعديل أو الإتلاف أو النسخ غير المصرح به أو تزوير المعلومات.

عرض محتوى الكتاب

أهمية الأمن السيبراني:



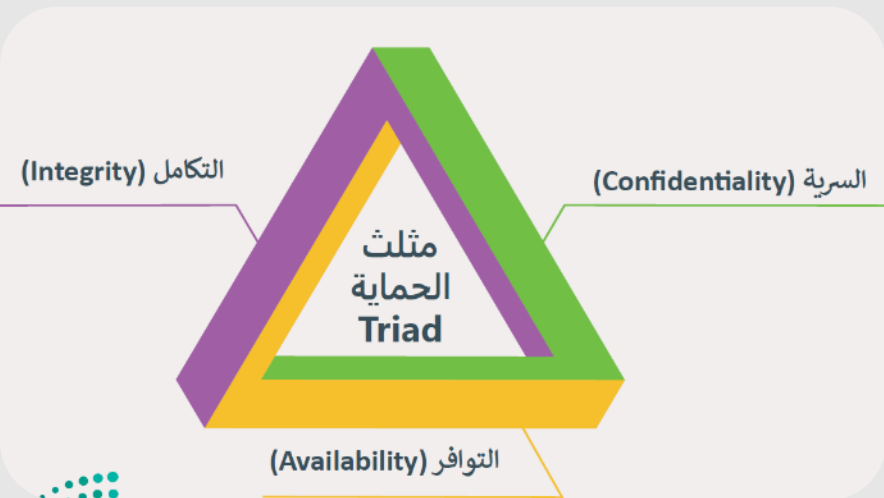
تزداد أهمية الأمن السيبراني بزيادة أهمية البيانات والمعلومات المتوفرة على الشبكة، وضرورة توافرها للمستخدمين دون انقطاع، بالإضافة إلى عدد المستخدمين الذين يحتاجون للوصول إلى تلك البيانات والمعلومات بشكل مستمر، وكلما زادت أهمية المعلومات كلما كانت عرضة لهجمات القرصنة الحاسوبية بهدف سرقتها أو حجبها عن المستخدمين وغير ذلك. يتمثل الدور المهم للأمن السيبراني في منع التهديدات الداخلية والخارجية واكتشافها والقيام بالاستجابة المناسبة لها حسب الضرورة.

عرض محتوى الكتاب

مثلث الحماية CIA:

01 السرية: السرية هي إتاحة البيانات والمعلومات للأشخاص المعنيين بها فقط والمسموح لهم بالاطلاع عليها، ولتحقيق ذلك يتم استخدام أساليب مختلفة مثل اسم المستخدم وكلمة المرور، وقوائم الأشخاص ذوي الصلاحيات.

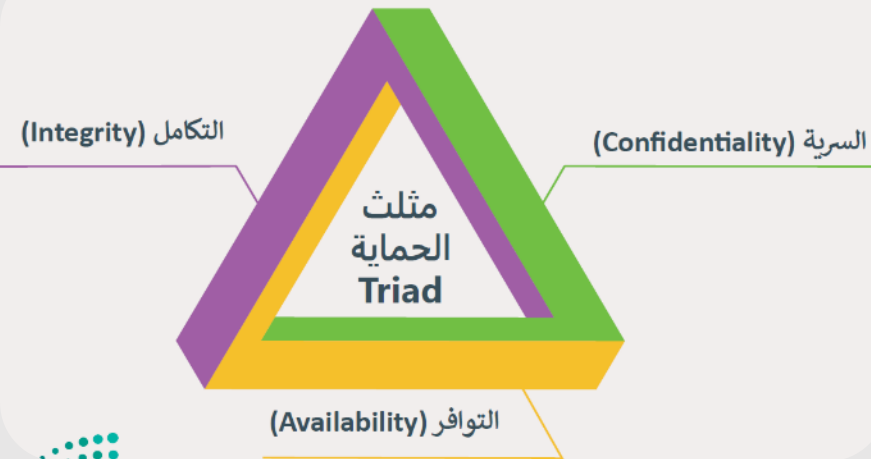
02 التكامل: يشير مصطلح التكامل إلى الحفاظ على دقة وصحة المعلومات، والتأكد من عدم إمكانية تعديلها إلا من قبل الأشخاص المخولين بذلك، ومن أساليب الحفاظ على تكامل البيانات والمعلومات: تحديد الأذونات والصلاحيات، والتشفير، وغيرها.



عرض محتوى الكتاب

مثلث الحماية CIA:

03 التوافر: التوافر يعني ضمان الوصول للمعلومات في الوقت المناسب وبطريقة موثوقة لاستخدامها، حيث إن أي نظام معلومات عليه توفير المعلومات عند الحاجة إليها وذلك ليؤدي الغرض الأساسي له. ومن أمثلة الإجراءات المتخذة لضمان توافر البيانات والمعلومات، الحفاظ على سلامة الأجهزة المستضيفة للبيانات، والنسخ الاحتياطي، وتحديثات النظام، وتحسين كفاءة الشبكة لتسهيل وصول المستخدمين ما أمكن.



عرض محتوى الكتاب

الجرائم الإلكترونية:

أنواع الجرائم الإلكترونية:



01 الاحتيال الإلكتروني: يحدث هذا الاحتيال عندما يتقمص المجرم الإلكتروني دور جهة موثوقة يتعامل معها الضحية، بغرض الحصول على معلومات شخصية عن مستخدم معين مثل كلمات المرور المصرفية وعنوان البيت أو الرقم الشخصي. تتم هذه العملية عادةً من خلال مواقع الاحتيال التي تُقلد المواقع الرسمية.

02 سرقة الهوية: بعد سرقة البيانات الشخصية، يقوم المحتالون بانتحال شخصية الضحية واستخدام بياناته لإجراء معاملات مالية، أو أعمال غير قانونية.

عرض محتوى الكتاب

الجرائم الإلكترونية: أنواع الجرائم الإلكترونية:

03 المضايقات عبر الإنترنت: تشمل التهديدات عبر البريد الإلكتروني أو الرسائل الفورية أو المشاركات المسيئة في وسائل التواصل الاجتماعي مثل فيسبوك وتويتر.

04 التسلل الإلكتروني: عادة ما يصيب المتسللون الإلكترونيون أجهزة الحاسب الخاصة بضحاياهم ببرامج ضارة يمكنها تسجيل نشاط الحاسب لمراقبة نشاطاتهم عبر الإنترنت، فمثلا يقوم برنامج مسجل المفاتيح بتتبع وتسجيل أضرار لوحة المفاتيح المضغوطة بطريقة سرية بحيث يصعب على الشخص معرفة أنه تتم مراقبته وجمع بياناته الخاصة.



عرض محتوى الكتاب

الجرائم الإلكترونية: أنواع الجرائم الإلكترونية:



05 انتهاك الخصوصية: يحدث انتهاك الخصوصية عند محاولة شخص ما التطفل على الحياة الشخصية لشخص آخر، وقد يتضمن ذلك اختراق الحاسب الشخصي الخاص به أو قراءة رسائل البريد الإلكتروني أو مراقبة الأنشطة الشخصية الخاصة به عبر الإنترنت.

عرض محتوى الكتاب

الاختراق الأمني:

أمثلة على الاختراقات في المؤسسات الكبيرة:



01 فيسبوك: في عام 2019 ، كشف باحثوا أمن المعلومات أن ملايين سجلات مستخدمي فيسبوك كانت منتشرة عبر الإنترنت، بسبب قيام بعض التطبيقات التي يسمح لها فيسبوك بالوصول إلى بيانات مستخدميه بتخزين تلك البيانات على خوادم خاصة بها دون وضع تدابير الأمان المطلوبة، وتم العثور على ملايين السجلات بما فيها معرفات المستخدمين على فيسبوك، التعليقات، الإعجابات، ردود الفعل وأسماء الحسابات في قاعدة بيانات تم تحميلها بواسطة الناشر الرقمي المكسيكي كولتورا كوليكثيفا الذي تم اكتشافه على الخوادم السحابية لخدمات أمازون ويب، وهذا يدعو إلى اتخاذ تدابير الحيلة والحذر قبل السماح لبرامج الأطراف الخارجية التي تصادفنا على منصات التواصل الاجتماعي بالوصول إلى معلوماتنا.

عرض محتوى الكتاب

الاختراق الأمني:

أمثلة على الاختراقات في المؤسسات الكبيرة:



02 ماريوت الدولية: في نوفمبر 2018 ، سرق لصوص الإنترنت بيانات ما يقارب 500 مليون عميل لشركة ماريوت الدولية، وتعتقد الشركة أن أرقام بطاقات الائتمان وتواريخ انتهاء الصلاحية لأكثر من 100 مليون عميل قد سُرقَت أيضًا، رغم أنه لم يكن من المؤكد فيما إذا تمكن المهاجمون من فك تشفير أرقام بطاقات الائتمان.

عرض محتوى الكتاب

الاختراق الأمني:

أمثلة على الاختراقات في المؤسسات الكبيرة:



03 جوجل+: في أكتوبر 2018 ، تم الإبلاغ عن اختراق مبدئي طال 500 ألف من مستخدمي جوجل+، ولكن شركة جوجل أعلنت عن الاختراق بعد عدة أشهر من اكتشافه. في ديسمبر، كشفت الشركة عن اختراق آخر للبيانات تم خلاله كشف المعلومات الشخصية لـ 52,5 مليون حساب على جوجل+ لمدة ستة أيام لتطبيقات غير جوجل+. تضمن هذا الاختراق بيانات مثل الأسماء، عناوين البريد الإلكتروني، تواريخ الميلاد ونوع المعلومات الشخصية الأخرى التي تم جمعها بواسطة جوجل+.

عرض محتوى الكتاب

الاختراق الأمني:

أمثلة على الاختراقات في المؤسسات الكبيرة:



04 تويتر: في عام 2019 ، قام مئات من مستخدمي تويتر عن غير قصد بإعطاء بياناتهم الشخصية لتطبيقات طرف ثالث. اعترفت الشركة بأنها أصدرت إصلاحًا لرمز خبيث ربما تم إدراجه في تطبيقها من قبل قراصنة الحاسب وكان من الممكن أن يعرض معلومات بعض المستخدمين في جميع أنحاء العالم للخطر. تم إعلام شركة تويتر بالمشكلة من قبل باحثي أمن تابعين لجهة ثالثة، اكتشفوا أن مجموعات تطوير برامج وان أودينس وموبي بيرن قد سمحت بالوصول إلى بيانات المستخدمين الحساسة. شملت المعلومات المكشوفة أسماء المستخدمين، عناوين البريد الإلكتروني والتغريدات الحديثة.

عرض محتوى الكتاب

الاختراق الأمني:

أمثلة على الاختراقات في المؤسسات الكبيرة:



05 أدوبي: أعلنت الشركة في البداية بأن المتسللين سرقوا ما يقارب 3 ملايين من سجلات بطاقات ائتمان العملاء المشفرة، بالإضافة إلى بيانات تسجيل الدخول لعدد غير محدد من حسابات المستخدمين، ولكن بعد أسابيع من البحث تم اكتشاف أن هذا الاختراق قد كشف عن الكثير من بيانات العملاء بما فيها مُعرِّفاتهم وكلمات المرور ومعلومات بطاقات الخصم وبطاقات الائتمان الخاصة بهم.

● مهارة التفكير



هل تطوير الأمن السيبراني مهم للحكومة؟
وضح ذلك؟





وزارة التعليم
Ministry of Education



النشاط الصفّي

اختر الإجابة الصحيحة

1- يتعلق مفهوم الأمن السيبراني بالحماية من الوصول غير المصرح به، لـ:

البرمجيات الضارة

أ

الشبكات

ب

التسلل الإلكتروني

ج



وزارة التعليم
Ministry of Education



النشاط الصفّي

اختر الإجابة الصحيحة

2- تضمن أنظمة الجاهزية العالية:

أ منع هجمات إيقاف الخدمة

أ

ب انقطاع التيار الكهربائي

ب

ج تعطيل الأجهزة

ج



وزارة التعليم
Ministry of Education



النشاط الصفّي

اختر الإجابة الصحيحة

3- من عناصر مثلث الحماية، ويعني ضمان الوصول للمعلومات في الوقت المناسب، وبطريقة موثوقة استخدامها:

السرية

أ

التكامل

ب

التوافر

ج



وزارة التعليم
Ministry of Education



النشاط الصفّي

اختر الإجابة الصحيحة

4- عملية تجاوز طرف غير مصرح به لتدابير الحماية،
للوصول إلى مناطق محمية في النظام، تسمى:

الأمن السيبراني

أ

الاختراق الأمني

ب

مثلث الحماية

ج



وزارة التعليم
Ministry of Education

ماذا تعلمنا خلال الدرس ؟





وزارة التعليم
Ministry of Education



الواجب المنزلي للمجموعة

١	تزداد أهمية الأمن السيبراني، في حالة:				
أ	البيانات غير المهمة	ب	قلة عدد المستخدمين	ج	ضرورة توافر البيانات
٢	من عناصر مثلث الحماية، ويشير إلى الحفاظ على دقة وصحة المعلومات:				
أ	السرية	ب	التكامل	ج	التوافر
٣	من أمثلة الإجراءات المتخذة لضمان توافر البيانات والمعلومات:				
أ	النسخ الاحتياطي	ب	قوائم الأشخاص ذوي الصلاحيات	ج	تحديد الأذونات
٤	الجريمة الإلكترونية التي يتقمص فيها المجرم الإلكتروني دور جهة موثوقة يتعامل معها الضحية، تسمى:				
أ	الاحتيال الإلكتروني	ب	سرقة الهوية	ج	التسلل الإلكتروني



وزارة التعليم
Ministry of Education

ختام الدصة الأولى



وزارة التعليم
Ministry of Education

بيانات الدرس



صفحات الكتاب

الحصة الثانية

من صفحة: 17

إلى صفحة: 20



عدد الحصص

حصتان



عنوان الدرس

مقدمة في الأمن
السيبراني



رقم الدرس

الدرس الأول



وزارة التعليم
Ministry of Education



الواجب
المنزلي
للمجموعة

اختر الإجابة الصحيحة

1- تزداد أهمية الأمن السيبراني، في حالة:

البيانات غير المهمة

أ

قلة عدد المستخدمين

ب

ضرورة توافر البيانات

ج



وزارة التعليم
Ministry of Education



الواجب
المنزلي
للمجموعة

اختر الإجابة الصحيحة

2- من عناصر مثلث الحماية، ويشير إلى الحفاظ على
دقة وصحة المعلومات:

السرية

أ

التكامل

ب

التوافر

ج



وزارة التعليم
Ministry of Education



الواجب
المنزلي
للمجموعة

اختر الإجابة الصحيحة

3- من أمثلة الإجراءات المتخذة لضمان توافر البيانات والمعلومات:

النسخ الاحتياطي

أ

قوائم الأشخاص ذوي الصلاحيات

ب

تحديد الأذونات

ج



وزارة التعليم
Ministry of Education



الواجب
المنزلي
للمجموعة

اختر الإجابة الصحيحة

4- الجريمة الإلكترونية التي يتقمص فيها المجرم الإلكتروني دور جهة موثوقة يتعامل معها الضحية، تسمى:

الاحتيال الإلكتروني

أ

سرقة الهوية

ب

التسلل الإلكتروني

ج



وزارة التعليم
Ministry of Education

الإستراتيجيات





وزارة التعليم
Ministry of Education



حيث يساعدنا في التعرف على
التحديات الرقمية المحيطة بنا

وتطوير مهارات الحماية الشخصية



النشاط الاثرائي





وزارة التعليم
Ministry of Education

مفردات الدرس

4 • الوقاية من الجرائم الإلكترونية

3 • هجوم الوسيط

2 • هجمات حجب الخدمات

1 • الهجمات الإلكترونية





وزارة التعليم
Ministry of Education

ماذا سنتعلم ؟

طرق الوقاية من
الجرائم
الإلكترونية.

أمثلة على
الوسيط
الإلكتروني.

هجوم
الوسيط.

مقارنة بين
هجمات حجب
الخدمات وحجب
الخدمات الموزع.

الهجمات
الإلكترونية.

مُخصر الدرس





وزارة التعليم
Ministry of Education



ورقة العمل

ثالث متوسط
١٤٤٨ هـ

مادة المهارات الرقمية

ص: ١٧ ٧- ما المقصود بالهجمات الإلكترونية؟

ص: ١٧ ٨- ما الفرق بين هجوم حجب الخدمات وهجوم حجب الخدمات الموزع؟

ص: ١٨ ٩- ما المقصود بهجوم الوسيط؟

ص: ١٨ ١٠- ما الأمثلة على هجوم الوسيط الإلكتروني؟

ص: ١٩ ١١- ما طرق الوقاية من الجرائم الإلكترونية؟

الجمعة الأولى

النشاط الصفّي

اسم المعلم / أ. /

عرض محتوى الكتاب

الهجمات الإلكترونية:



الهجمات الإلكترونية هي محاولات لسرقة المعلومات، أو كشفها، أو تعطيلها، أو إتلافها من خلال الوصول غير المصرح به إلى جهاز الحاسب. وهي أيضًا محاولة للوصول غير المصرح به إلى نظام الحوسبة أو شبكة الحاسب بقصد إحداث ضرر. عادة ما يتم تنفيذ الهجمات الإلكترونية بطريقة غير قانونية وبنية إحداث ضرر، ويمكن أن يكون لها عواقب وخيمة على المهاجمين.

عرض محتوى الكتاب

هجمات حجب الخدمات وحجب الخدمات الموزع:



01 هجوم حجب الخدمات: هجوم حجب الخدمات هو نوع من أنواع الهجمات السيبرانية حيث يقوم جهاز حاسب واحد أو شبكة بإغراق موقع أو خادم مستهدف بحركة المرور، مما يؤدي إلى إرباكه وجعله غير متاح للمستخدمين.

02 هجوم حجب الخدمات الموزع: هجوم حجب الخدمات الموزع هو إصدار أكثر تقدمًا من هجوم حجب الخدمات حيث يتم استخدام العديد من أجهزة الحاسب أو الشبكات لإغراق موقع ويب أو خادم مستهدف بحركة المرور، مما يجعل الدفاع ضده أكثر صعوبة. تجعل المصادر المتعددة لحركة المرور من الصعب منع الهجوم؛ لأنه يبدو أنه قادم من مواقع متعددة.

عرض محتوى الكتاب

هجمات حجب الخدمات وحجب الخدمات الموزع:



03 هجوم الوسيط: هجوم الوسيط هو نوع من الهجمات الإلكترونية يتطفل فيه المهاجم بين اتصال المستخدم والتطبيق، ويجلس في منتصفه متظاهراً بأنه الطرف الآخر، ويمكنه قراءة أو تعديل أو إدخال رسائل جديدة في تدفق الاتصال. يمكن استخدام هجوم الوسيط لسرقة معلومات حساسة أو نشر برامج ضارة أو تنفيذ أنشطة ضارة أخرى. يمكن التخفيف من هذه الهجمات باستخدام أساليب التشفير والمصادقة.

عرض محتوى الكتاب

هجمات حجب الخدمات وحجب الخدمات الموزعة: أمثلة على هجومات الوسيط الإلكتروني:



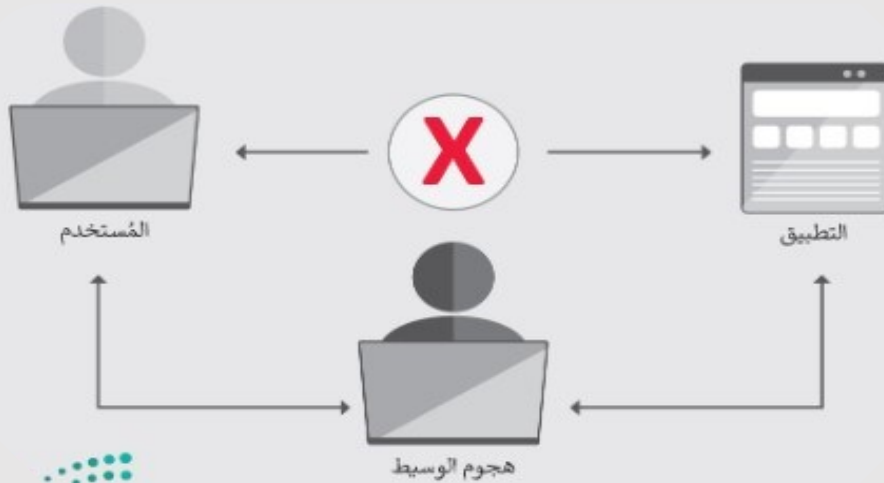
01 التنصت على الواي فاي: يمكن للمهاجم إعداد نقطة وصول واي فاي خادعة تظهر على أنها نقطة وصول شرعية، مما يسمح له باعتراض وقراءة حركة مرور الشبكة غير المشفرة المرسلة من قبل الضحايا المطمئنين الذين يتصلون بنقطة الوصول الخادعة.

02 انتحال أسماء النطاقات: في هذا الهجوم، يعترض المهاجم استعلامات نظام اسم النطاق DNS ويغيرها، ويعيد توجيه الضحايا إلى موقع ويب ضار بدلاً من موقع الويب المشروع المقصود.

عرض محتوى الكتاب

أمثلة على هجوم الوسيط الإلكتروني:

03 التصيد الاحتيالي للبريد الإلكتروني: في هذا النوع من الهجوم يعترض المهاجم رسائل البريد الإلكتروني وتغيير المحتوى أو إضافة مرفقات أو روابط ضارة لسرقة معلومات حساسة أو لنشر برامج ضارة.

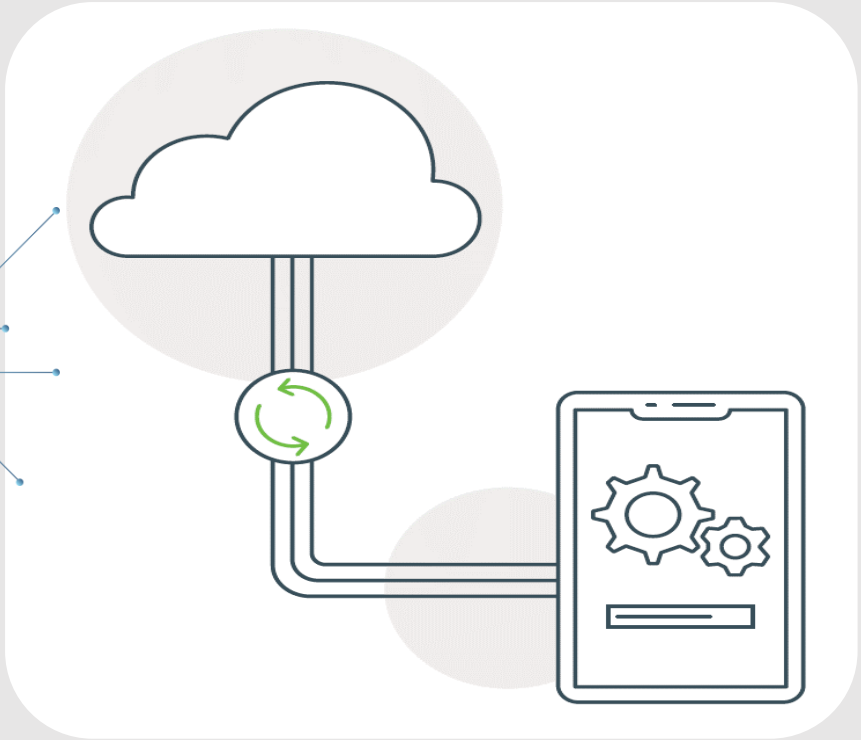


عرض محتوى الكتاب

الوقاية من الجرائم الإلكترونية:

بعض التدابير التي تنصح باتخاذها للوقاية من الجرائم الإلكترونية:

01 التحديث الدوري للبرامج: يُعدُّ تحديث البرمجيات أحد أكثر حلول الأمن السيبراني للتقليل من خطر برمجيات الاختراق الخاصة وخاصة تلك التي تعتمد على ابتزاز المستخدم، يجب أن يشمل هذا التحديث المستمر كلاً من نظام التشغيل والتطبيقات، وذلك لإزالة الثغرات الأمنية الحرجة التي قد يستخدمها المتسللون للوصول إلى الأجهزة الثابتة والمحمولة والهواتف الذكية.



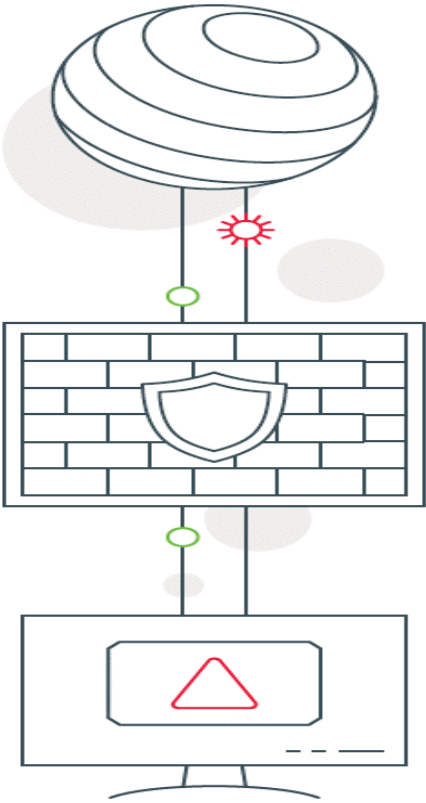
عرض محتوى الكتاب

الوقاية من الجرائم الإلكترونية:

بعض التدابير التي تنصح باتخاذها للوقاية من الجرائم الإلكترونية:

02 استخدام برامج مكافحة الفيروسات وجدار الحماية: يُعدُّ برنامج مكافحة الفيروسات الحل الأكثر نجاحًا في محاربة الهجمات؛ نظرًا لأنه يمنع البرمجيات الضارة والفيروسات الخبيثة الأخرى من الدخول إلى جهازك وتعرض بياناتك للخطر، ويُعدُّ استخدام برنامج حماية مناسب مهمًا في الحفاظ على بياناتك من الهجمات، فهو يساعد على حجب المتسللين والفيروسات والنشاطات الضارة الأخرى عبر الإنترنت وتحديد وتقنين البيانات المسموح بمرورها إلى جهازك.

يتحكم جدار الحماية في حركة مرور البيانات الواردة والصادرة من خلال تحليل حزم البيانات وتحديد ما إذا كان ينبغي السماح بمرورها أم لا. وقد تأتي جدر الحماية على صورة برامج يتم تثبيتها على أجهزة الحاسب بشكل فردي، أو على شكل أجهزة خارجية منفصلة تستخدم ضمن هيكل الشبكة لحمايتها من الهجمات الخارجية. يمكن لبرامج جدار الحماية المثبتة على أجهزة الحاسب الفردية أن تفحص البيانات عن كثب، ويمكن أن تمنع برامج محددة من إرسال البيانات إلى الإنترنت. تستخدم الشبكات ذات الاحتياطات الأمنية العالية كلا النوعين من جدران الحماية لتأمين شبكة أمان كاملة.



عرض محتوى الكتاب

الوقاية من الجرائم الإلكترونية:

بعض التدابير التي تنصح باتخاذها للوقاية من الجرائم الإلكترونية:

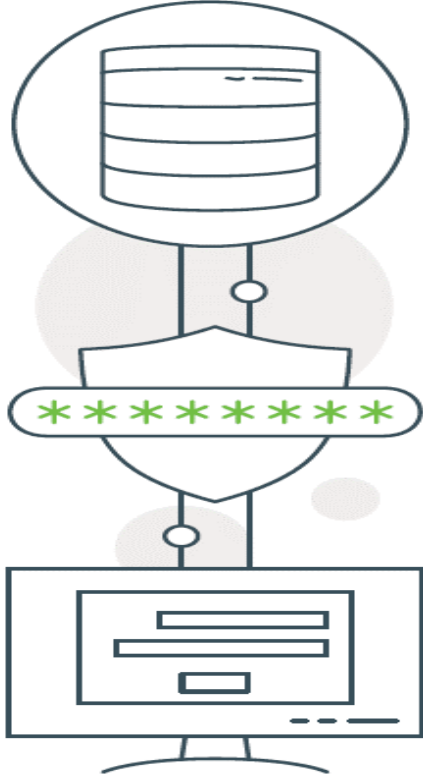
03 التواصل الرقمي الحذر: الانتباه إلى كافة أشكال التواصل الرقمي سواء عبر البريد الإلكتروني أو منصات التواصل الاجتماعية وحتى المكالمات الهاتفية والرسائل النصية. فمثلاً تجنب فتح الرسائل الإلكترونية المرسلة من جهات مجهولة، والتأكد من الروابط التشعبية بدقة قبل الضغط عليها، وتوخي الحذر من مشاركة أي معلومات شخصية عبر هذه المنصات.



عرض محتوى الكتاب

الوقاية من الجرائم الإلكترونية:

بعض التدابير التي تنصح باتخاذها للوقاية من الجرائم الإلكترونية:



04 استخدام كلمات المرور القوية وأدوات كلمات المرور: يُعدُّ استخدام كلمات المرور القوية أمرًا ضروريًا مهمًّا لاعتبارات الأمن عبر الإنترنت، ووفقًا لسياسة استخدام كلمات المرور الجديدة، يجب أن تكون كلمة المرور القوية على درجة كافية من التعقيد، وتتغير بشكل دوري. وفي هذا الوقت الذي تتعدد حسابات المستخدمين على منصات وتطبيقات عديدة، ظهرت الحاجة إلى استخدام أدوات إدارة كلمات المرور والتي تحتفظ بكلمات المرور بصورة مشفرة في قواعد بيانات آمنة، بحيث يتم استرجاعها عند طلب المستخدم والتحقق من هويته.

عرض محتوى الكتاب

الوقاية من الجرائم الإلكترونية:

بعض التدابير التي تنصح باتخاذها للوقاية من الجرائم الإلكترونية:

05 التحقق الثنائي أو المتعدد: تقدم عملية التحقق الثنائي أو المتعدد خيارات أمان إضافية، حيث تتطلب عملية المصادقة التقليدية إدخال اسم المستخدم وكلمة المرور فقط، بينما يتطلب التحقق الثنائي استخدام طريقة إضافية كرمز التعريف الشخصي أو كلمة مرور أخرى أو حتى استخدام بصمة الإصبع. أما استخدام التحقق متعدد العوامل فيطلب أكثر من طريقتين. تتضمن أمثلة التحقق الثنائي أو المتعدد استخدام مزيج من هذه العناصر للمصادقة مثل: الرموز الناتجة عن تطبيقات الهواتف الذكية، البطاقات أو أجهزة USB أو الأجهزة المادية الأخرى، بصمات الأصابع، الرموز المرسلة إلى عنوان بريد إلكتروني، التعرف على الوجه وإجابات لأسئلة الأمان الشخصي.



عرض محتوى الكتاب

الوقاية من الجرائم الإلكترونية:

بعض التدابير التي تنصح باتخاذها للوقاية من الجرائم الإلكترونية:



06 النسخ الاحتياطي الدوري للبيانات: يعد إجراء نسخ احتياطي للبيانات بشكل دوري خطوة مهمة في مجال الحفاظ على أمان الإنترنت الشخصي، فبشكل أساسي عليك الاحتفاظ بثلاث نسخ من بياناتك على نوعين مختلفين من وسائط تخزين البيانات، كنسختين على (القرص الصلب المحلي والخارجي)، ونسخة أخرى على موقع خارجي أو باستخدام التخزين السحابي. في حالة استهدافك بالبرمجيات الضارة تكون الطريقة الوحيدة لاستعادة البيانات هي باستعادة آخر نسخة احتياطية كبديل عن النظام الحالي المصاب بالبرمجيات الضارة.

عرض محتوى الكتاب

الوقاية من الجرائم الإلكترونية:

بعض التدابير التي تنصح باتخاذها للوقاية من الجرائم الإلكترونية:

07 تجنب استخدام شبكات واي فاي العامة: ينصح بتجنب استخدام شبكة واي فاي العامة دون استخدام شبكة افتراضية خاصة، فباستخدام هذه الشبكة، يتم تشفير حركة نقل البيانات بين الجهاز وخادم VPN مما يصعب على القرصنة الوصول إلى بياناتك على الإنترنت، كما يوصى باستخدام الشبكة الخلوية عند عدم وجود شبكة VPN وذلك للحصول على مستوى أعلى من الأمان.



● مهارة التفكير



لماذا تنشط الهجمات الإلكترونية وقت
الحروب؟





وزارة التعليم
Ministry of Education



النشاط الصفّي

اختر الإجابة الصحيحة

1- محاولات سرقة المعلومات، أو كشفها، وتعطيها،
تسمى:

مثث الحماية

أ

الهجمات الإلكترونية

ب

الأمن السيبراني

ج



وزارة التعليم
Ministry of Education



النشاط الصفّي

اختر الإجابة الصحيحة

2- هجوم إلكتروني يؤدي إلى إغراق موقع أو خادم
مستهدف بحركة المرور، مما يؤدي إلى جعله غير متاح
للمستخدمين:

هجوم حجب الخدمات

أ

هجوم حجب الخدمات الموزع

ب

الاختيال الإلكتروني

ج



وزارة التعليم
Ministry of Education



النشاط الصفى

اختر الإجابة الصحيحة

3- نوع من الهجمات الإلكترونية يتطفل فيه المهاجم بين اتصال المستخدم والتطبيق، هو:

سُرقة الهوية

أ

برامج مكافحة الفيروسات

ب

هجوم الوسيط

ج



وزارة التعليم
Ministry of Education



النشاط الصفّي

اختر الإجابة الصحيحة

4- من التدابير التي ينصح باتخاذها للوقاية من الجرائم الإلكترونية:

زيارة مواقع إلكترونية مجهولة

أ

التواصل الرقمي الحذر

ب

استخدام شبكات واي فاي العامة

ج



وزارة التعليم
Ministry of Education

ماذا تعلمنا خلال الدرس ؟



خريطة مفاهيم

مقدمة في الأمن السيبراني



المفهوم الرئيسي

يتعلق الأمن السيبراني بحماية أجهزة الحاسب والشبكات والبرامج والبيانات من الوصول غير المصرح به، بهدف منع سرقة المعلومات الحساسة أو تغييرها أو إتلافها أو ابتزاز المستخدمين أو تعطيل الأعمال.

الأمن السيبراني

- التعريف: حماية الأنظمة والبيانات من التهديدات الرقمية.
- النطاق: يشمل الأجهزة والشبكات والبرامج والحسابات.
- الهدف: تقليل المخاطر وتعزيز الأمان الرقمي.

أهمية الأمن السيبراني

- الخصوصية: حماية معلومات الأفراد والمؤسسات.
- استمرارية العمل: تقليل التوقف والخسائر.
- الثقة: تعزيز موثوقية الخدمات الرقمية.

مثلث الحماية CIA

- السرية: منع وصول غير المصرح لهم إلى البيانات.
- السلامة: الحفاظ على دقة البيانات وعدم العبث بها.
- الإتاحة: ضمان وصول المستخدم المصرح له عند الحاجة.

الجرائم الإلكترونية

- المفهوم: أفعال غير قانونية تُرتكب باستخدام التقنية.
- الأهداف: سرقة بيانات أو أموال أو تعطيل خدمات.
- الأثر: خسائر مادية ومعنوية وتشغيلية.

أنواع الجرائم الإلكترونية

- التصيد الاحتيالي: رسائل أو صفحات مزيفة لسرقة البيانات.
- البرمجيات الخبيثة: فيروسات وبرامج ضارة تهاجم الأجهزة.
- سرقة الهوية: انتحال شخصية المستخدم واستغلال معلوماته.
- الابتزاز الرقمي: تهديد الضحية بمقابل المال أو البيانات.

طرق الوقاية من الجرائم الإلكترونية

- استخدام مضاد فيروسات ونسخ احتياطي وعدم مشاركة البيانات الحساسة.
- الحذر من الروابط والمرفقات والرسائل المشبوهة.
- تحديث الأنظمة والبرامج بانتظام.
- كلمات مرور قوية وتفعيل التحقق الثنائي.

خلاصة

الوعي بالمخاطر والدلائل م بإجراءات الحماية الرقمية يساعدان على تقليل الجرائم الإلكترونية وحماية البيانات.

6

الاختراق الأمني



- المفهوم: دخول غير مصرح به إلى نظام أو حساب.
- الأسباب: كلمات مرور ضعيفة أو ثغرات أو إهمال.
- النتائج: تسريب بيانات أو حذفها أو تعطيل النظام.

7

الهجمات الإلكترونية



- أنواع شائعة: تصيد، برمجيات فدية، برمجيات خبيثة، حجب خدمة.
- الوسائل: استغلال الثغرات أو الروابط والملفات الضارة.
- النتيجة: إرباك الخدمات أو فقدان البيانات أو الابتزاز.

8

مقارنة بين هجمات حجب الخدمات وحجب الخدمات الموزع



- DoS: الهجوم يأتي من مصدر واحد.
- DDoS: الهجوم يأتي من عدة أجهزة في وقت واحد.
- التأثير: DDoS، أشد وأصعب في الإيقاف.
- الهدف: إبطاء الخدمة أو إيقافها عن المستخدمين.

9

هجوم الوسيط



- المفهوم: اعتراض الاتصال بين طرفين دون علمهما.
- كيف يحدث: التنصت أو إعادة التوجيه أثناء تبادل البيانات.
- الهدف: سرقة معلومات مثل كلمات المرور والبيانات المالية.

10

أمثلة على الوسيط الإلكتروني



- شبكة واي فاي مزيفة في مكان عام.
- اعتراض جلسة تسجيل الدخول على شبكة غير آمنة.
- تبديل البيانات أثناء التصفح أو الدفع الإلكتروني.

11

طرق الوقاية من الجرائم الإلكترونية



- كلمات مرور قوية وتفعيل التحقق الثنائي.
- تحديث الأنظمة والبرامج بانتظام.
- الحذر من الروابط والمرفقات والرسائل المشبوهة.
- استخدام مضاد فيروسات ونسخ احتياطي وعدم مشاركة البيانات الحساسة.



الواجب المنزلي

للمجموعة

التقويم النهائي

الاسم: الصف:

ضع علامة (✓) أمام الإجابة الصحيحة:

١	الأمن السيبراني هو:
☐	أ حماية الأجهزة والبيانات من الوصول غير المصرح به
☐	ب برنامج رسم
☐	ج جهاز
☐	د لعبة
٢	الجريمة الإلكترونية (Cybercrime) هي:
☐	أ برنامج مفيد
☐	ب استخدام الحاسب لتحقيق غايات غير قانونية
☐	ج جهاز
☐	د تخزين
٣	من أمثلة الجرائم الإلكترونية:
☐	أ الطباعة
☐	ب الحفظ
☐	ج الاحتيال وسرقة الهوية
☐	د الرسم
٤	الهجوم الذي يتطغل فيه المهاجم بين المستخدم والتطبيق يُسمَّى:
☐	أ الطباعة
☐	ب الحفظ
☐	ج الرسم
☐	د هجوم الوسيط (MitM)
٥	إتاحة البيانات للأشخاص المعنيين بها فقط هو مفهوم:
☐	أ السرية (Confidentiality)
☐	ب الطباعة
☐	ج الحذف
☐	د التكبير



وزارة التعليم
Ministry of Education

مشروع الوحدة الأولى

صفحة رقم: 41

الطرح والمناقشة

- تعريف الطلبة بالمشروع وخطواته.
- عرض فكرة المشروع وأهدافه المرتبطة بالوحدة.
- توضيح خطوات التنفيذ ومعايير التقييم.
- تقسيم الطلبة إلى مجموعات أو تكليف فردي
- تحديد زمن التنفيذ وجدول المتابعة وموعد التسليم.

بالتعاون مع مجموعة من زملائك في الصف، وبالبحث في المواقع الموثوقة؛ قدم عرضًا تقديميًا حول أحد الموضوعات الآتية:

الأمن السيبراني ونصائح للبقاء آمنًا عند الاتصال بالإنترنت، ويمكنك زيارة موقع العطاء الرقمي <https://attaa.sa>. وتصفح مكتبة الموقع الإلكتروني، وتصفح سلسلة فيديو بودكاست تسمى سايبير إكس، للبحث عن معلومات حول الأمن السيبراني. ستجد معلومات مفيدة حول مخطط المعلومات المرفق في المقالة، صمم عرضك التقديمي مع تسليط الضوء على الخطوات البسيطة التي يمكن لشخص ما أن يتخذها للبقاء آمنًا عند الاتصال بالإنترنت.

التنمر الإلكتروني وطرق تجنبه، ويمكنك زيارة الموقع الإلكتروني <https://thinktech.sa>. وتصفح موضوعات المدونة المتاحة. ومن قسم الفعاليات اختر موضوع التنمر الإلكتروني وتعزيز الصحة النفسية، وشاهد مقاطع الفيديو المتوفرة، واجمع المعلومات المناسبة لموضوع بحثك وقدمها في عرضك التقديمي مع نصائح لزملائك حول كيفية مواجهتها والحماية منها.

الجرائم الإلكترونية وكيفية الحماية منها، ويمكنك زيارة موقع الهيئة الوطنية للأمن السيبراني <https://www.nca.gov.sa>. للبحث عن معلومات حول الجريمة الإلكترونية وأمثلة محتملة لها. وعن النموذج الذي يمكنك استخدامه للإبلاغ عن الجرائم الإلكترونية، وأضفها في العرض التقديمي الخاص بك، وقدم نصائح لزملائك للحماية من هذه الجرائم والإبلاغ عنها عند التعرض لها.

صمم عرضك التقديمي مع مراعاة الجوانب الجمالية عند التصميم، وإضافة الصورة المناسبة لموضوع بحثك، وتوثيق مصادرك.

قدم عرضك وناقش زملاءك في الصف حول المعلومات الواردة فيه، ثم عدله بناءً على نتائج المناقشة وارفعه لمعلمك عبر البريد الإلكتروني.



همسات توعوية



وزارة التعليم
Ministry of Education

من خلال عنوان الدرس

مقدمة في الأمن السيبراني

نقوم بتعبئة الخانتين على اليسار



كيف أتعلم المزيد؟



ماذا تعلمت؟



ماذا أريد أن أعرف؟



ماذا أعرف؟



وزارة التعليم
Ministry of Education

ختام الدرس

